2

Updated Final Report to Office of Naval Research
Contract N00014-86-K-0507
December 3, 1990

"Behavior-Based Fault Monitoring"

Principal Investigator: **John P. Shen**

Center for Dependable Systems
Department of Electrical and Computer Engineering
Carnegie Mellon University
Schenley Park, Pittsburgh PA 15213
(412) 268-3601
INTERNET address: shen@ece.cmu.edu

Abstract

An approach is developed which exploits the deterministic behavior of a processor to perform concurrent fault monitoring. A very low cost and highly effective technique, called Continuous Signature Monitoring (CSM), has been developed. This technique is capable of detecting transients with very low detection latency, and requires very minimal memory overhead and performance penalty. This technique has been applied to both CISC and RISC type processors. Both analytical and experimental results have been obtained in validating the effectiveness of the approach. CSM has been adopted by two aerospace companies in their design of a 32-bit RISC processor targeted for avionics and space applications. It appears that the signature monitoring technique can be extended to detect computer viruses as well via a form of program encryption.

I. Summary of Accomplishments

This section presents the technical motivations for fault monitoring, summarizes our signature monitoring technique called Continuous Signature Monitoring, and compares our results with other techniques. A list of publications resulting from our current contract is provided.

1. Motivation for Behavior-Based Monitoring

Concurrent error detection is necessary to ensure reliable computer operation. Although permanent hardware faults can be detected using built-in self-test (BIST) or an external tester, concurrent detection must be used to detect errors caused by transient faults. Based on a number of experimental studies, transient faults constitute the dominant fault type in most systems during system operation.

Traditional approaches to concurrent error detection add redundancy based on a computer's structure. The most common approach is structural duplication. Although effective, duplication is too expensive for all but a few applications. Redundancy can also be incorporated via the use of error checking codes. However, most techniques based on error checking codes are only effective against very specific error types, e.g. single or double bit errors.

We propose an approach to concurrent error detection, or fault monitoring, in processors which uses behavioral abstraction of the executing program that is monitored for run-time violations. Such behavior-based approach has the advantage that errors from any source are potentially detectable, including software and hardware design faults, as well as permanent and transient faults. Abstractions can be formed using various aspects of program behavior, including control flow, memory access, input-output, and object type or range. Experimental comparison of various abstractions shows that processor control flow offers the most error-detection potential. A number of researchers have proposed techniques that detect control-flow related errors using a simple monitor and signatured programs. We called these *signature monitoring* techniques.

2. Continuous Signature Monitoring

During the past several years, we have developed a new signature monitoring approach for processor fault monitoring that uses a simple hardware monitor and signatures embedded into the executing program. Signature-monitoring techniques detect a large portion of processor control errors at a fraction of the cost of duplication. Analytical methods developed in this work show that the new approach, Continuous Signature Monitoring (CSM), makes major advances beyond existing techniques.

A signature-monitoring technique's effectiveness can be characterized by five properties: (1) error-detection coverage, (2) memory overhead, (3) processor-performance loss, (4) error-detection latency, and (5) monitor complexity. Existing signature-monitoring techniques improve upon the original basic technique in one or more of these properties. However, all of the proposed improvements degrade one or more of the other properties. CSM approach makes major improvements in all signature-monitoring properties.

CSM reduces the fraction of undetected control-flow errors by orders of magnitude, to less than 10^{-6}. The number of signatures reaches a theoretical minimum, lowered by as much as three times to a range of 4-11%. Signature cost is reduced by placing CSM signatures at locations that minimize performance loss and, for some architectures, memory overhead. CSM exploits the program memory's SEC/DED code to decrease average error-detection latency by as much as 1000 times, to 0.016 program memory cycles, without increasing memory overhead. This short latency facilitates quick recovery in the tolerance of transient faults.

Figure 1 below compares the effectiveness of the CSM technique with three other signature monitoring techniques. The basic technique is the technique originally proposed. Path Signature Analysis (PSA) was developed at Stanford. The Signatured Instruction Streams (SIS) technique was developed at CMU and is the predecessor to the current CSM technique.

	Basic	PSA	SIS	CSM
Total Memory Overhead	10-25%	12-21%	6-15%	4-11%
Latency in PM Cycles	2-5	7-17	7-17	0.016-1.0
Control-Flow Error Coverage	96-99%	99.5-99.9%	85-93%	99.9999%
Control-Bit Error Coverage	99.9999%	100%	85-93%	99.9999%

Figure 1. Comparison of CSM to Other Signature Monitoring Techniques.

3. Resulting Publications

1. M.A. Schuette, J.P. Shen, D.P. Siewiorek and Y.X. Zhu, "An Experimental Evaluation of Two Concurrent Error Detection Approaches," ***Proc. of 16th Int. Fault Tolerant Computing Symp.***, July 1986.
2. J.P. Shen and M.A. Schuette, "Processor Control Flow Monitoring Using Signatured Instruction Streams," ***IEEE Trans. on Computers***, March 1987.
3. J.P. Shen and S.P. Tomas, "A Roving Monitoring Processor for Detection of Control Flow Errors in Multiple Processor Systems," ***Microprocessing and Microprogramming: The Euromicro Journal***, Special Issue on Fault Tolerant Computing, North-Holland, May 1987.
4. K.D. Wilken and J.P. Shen, "Embedded Signature Monitoring: Analysis and Techniques," ***Proc. of Int. Test Conf.***, September 1987.
5. K.D. Wilken and J.P. Shen, "Continuous Signature Monitoring: Efficient Concurrent-Detection of Processor Control Errors," ***Proc. of Int. Test Conf.***, September 1988.
6. K.D. Wilken and J.P. Shen, "Concurrent Error Detection Using Signature Monitoring and Encryption," ***Int. Conf. on Dependable Computing for Critical Applications***, August 1989.
7. K.D. Wilken and J.P. Shen, "Continuous Signature Monitoring: Efficient Concurrent Detection of Processor Control Errors," ***IEEE Trans. on Computer Aided Design***, June 1990.
8. K.D. Wilken and J.P. Shen, "Detecting Processor Hardware Errors and Computer Viruses Using Program Encryption and Signature Monitoring," submitted to ***IEEE Trans. on Computers***, 1990.

II. Presentation of Technical Results

This section is a compendium of major papers published through the support of this research contract. These papers document the key results of our research on Continuous Signature Monitoring as well as our earlier work on Signatured Instruction Streams. In total, three journal papers and four conference papers have resulted from this work. One more paper on extending CSM to cover a more generalized fault model and to detect computer viruses has been submitted to IEEE Transactions on Computers.